IAP16 Rec'd PCT/PTO 25 SEP 2006
10/594169

Verfahren zur Überwachung der Übertragung von elektronischen Nachrichten

Die Erfindung betrifft ein Verfahren zur computergestützten Überwachung der Übertragung von elektronischen Nachrichten innerhalb eines Datennetzwerkes. Gemäß dem Verfahren wird zunächst eine Absender-Identifikationsangabe einer eingehenden elektronischen Nachricht ermittelt. Daraufhin wird eine elektronische Datenbank abgefragt und es wird überprüft, ob die Absender-Identifikationsangabe in der Datenbank als akzeptable oder nicht-akzeptable Absender-Identifikationsangabe registriert ist. Schließlich wird die eingehende elektronische Nachricht in Abhängigkeit vom Ergebnis der Überprüfung übermittelt.

Die Kommunikation mittels elektronischer Nachrichten, so genannter E-Mails, die über das Internet oder ein sonstiges Datennetzwerk innerhalb eines Unternehmens oder auch weltweit übermittelt werden, ist heutzutage üblich. Wesentliche Vorteile der Kommunikation mittels E-Mails sind die hohe Geschwindigkeit der Informationsübermittlung sowie die geringen Kosten.

Die hohe Verfügbarkeit und die geringen Kosten haben aber in jüngerer Zeit dazu geführt, dass das Medium E-Mail zunehmend auch zur Verbreitung von Werbung genutzt wird. In zunehmendem Maße erhalten Internetnutzer daher unangeforderte E-Mails, die massenhaft von so genannten "Spammern" hauptsächlich zu Werbezwecken versandt werden. Spammer haben verschiedene Techniken zur Verfügung, um Informationen hinsichtlich der Empfänger-Identifikationsangaben, d. h. der E-Mail-Adressen, von potenziellen Spam-Empfängern zu erhalten. Hierzu werden beispielsweise automatisch

BESTÄTIGUNGSKOPIE

einschlägige Internetseiten, wie beispielsweise Nachrichtenseiten ("Newsgroup-Sites"), Internet-Foren ("Chat-Room-Sites"), Daten aus so genannten Mailinglisten oder sonst wie im Internet abrufbare E-Mail-Adressen abgefragt. Mit solchen Methoden gelangen die Spammer effektiv an E-Mail-Adressen, die dann als Ziel für Werbung oder sonstige unerwünschte elektronische Nachrichten genutzt werden.

Sehr zum Ärgernis der meisten Internetnutzer werden deren elektronische Postfächer zunehmend mit "Spam", d. h. unerwünschten elektronischen Nachrichten der beschriebenen Art, überschwemmt. Es ist mit Zeitaufwand verbunden, die unerwünschten Nachrichten auszusortieren und zu löschen. Außerdem wird durch die Übermittlung von Spam an die entsprechenden Empfänger Übertragungsbandbreite verschwendet, was Kosten auf Seiten der Empfänger, die für die Datenübertragung Gebühren an ihre Internet-Diensteanbieter zahlen, verursacht. Auch für die Internet-Diensteanbieter (Internet Service Provider) selbst, wie z. B. AOL, T-online usw., ist Spam ein schwerwiegendes Problem, da deren Kunden aufgrund der zuvor geschilderten Nachteile unzufrieden sind.

Bereits heute existieren verschieden Techniken zur Verhinderung und zur Blockierung von Spam. Entsprechende Programme, die die Übertragung von elektronischen Nachrichten über Datennetzwerke überwachen, werden auch als Spam-Filter bezeichnet. Eine bekannte Kategorie von Spam-Filtern arbeitet mit so genannten weißen Listen. Bei diesen weißen Listen handelt es sich um elektronische Datenbanken, in denen akzeptable Absender-Identifikationsangaben für die Übertragung von elektronischen Nachrichten gespeichert sind. Bei solchen Spam-Filtern wird zunächst die Absender-Identifikationsangabe, d. h. die E-Mail-Adresse, des Absenders einer eingehenden elektronischen Nachricht, ermittelt. Diese Absenderadresse wird dann mit den in der weißen Liste gespeicherten Adressen verglichen. Falls die Adresse in der weißen Liste als akzeptable Adresse registriert ist, wird die eingehende elektronische Nachricht an den entsprechenden Empfänger weitergeleitet. Gegebenenfalls kann jedem individuellen Empfänger von elektronischen Nachrichten eine eigene weiße Liste zugeordnet sein. Es ist aber auch bekannt, umfassende Datenbanken mit akzeptablen Absenderadressen, beispielsweise

für sämtliche Kunden eines Internet-Diensteanbieters, zu verwenden. Ebenso bekannt ist die Verwendung von schwarzen Listen, d. h. von Datenbanken, die ausschließlich nicht-akzeptable Absender-Identifikationsangaben enthalten. In den schwarzen Listen sind somit die Absenderadressen von bekannten Spam-Versendern registriert. Von diesen Spammern abgesandte Nachrichten werden dann automatisch erkannt und blockiert.

Die nach dem beschriebenen Verfahren der weißen Listen arbeitenden Spam-Filter haben eine Reihe von Nachteilen. Ein wesentlicher Nachteil resultiert daraus, dass häufig E-Mails irrtümlich als Spam identifiziert werden, obwohl es sich tatsächlich nicht um unerwünschte Nachrichten handelt. Dies führt dazu, dass die entsprechenden Nachrichten fälschlicherweise nicht zu deren Empfängern gelangen. Der Grund dafür ist, dass, wie zuvor beschrieben, nur solche E-Mails zugestellt werden, deren Absender als akzeptabel gelistet sind. Bei mit weißen Listen arbeitenden Spam-Filtern wird die Datenbank mit den akzeptablen Absenderadressen üblicherweise so generiert, dass bei Eingang einer E-Mail von einem bis dato unbekannten Absender dieser Absender automatisch eine von dem Spam-Filter generierte Antwort-Nachricht erhält, welche wiederum von dem Absender der im Spam-Verdacht stehenden Nachricht bestätigt werden muss. Wenn dann die Bestätigung eingeht, wird die Absenderadresse automatisch in die weiße Liste aufgenommen, und die ursprünglich eingegangene E-Mail wird ordnungsgemäß zugestellt. Problematisch ist dabei zum einen, dass einige Spammer mittlerweile dazu übergehen, von Spam-Filtern automatisch generierte Bestätigungs-Nachrichten ebenso automatisch zu beantworten, sodass dadurch das Spam-Filter umgangen wird. Ein weiterer Nachteil ist, dass bestimmte erwünschte elektronische Nachrichten derartige mit weißen Listen arbeitende Spam-Filter niemals passieren können. Dies betrifft beispielsweise E-Mails, die an die Abonnenten von so genannten Mailinglisten verschickt werden. Die Versender von Nachrichten an die Abonnenten von Mailinglisten beantworten nämlich in der Regel die Bestätigungs-Nachrichten des Spam-Filters nicht. Ebenso blockiert werden durchaus erwünschte E-Mails, die von Internet-Servern automatisch generiert werden, wie beispielsweise Bestellbestätigungen im Zusammenhang mit E-Commerce-Geschäften.

Davon ausgehend liegt der vorliegenden Erfindung die Aufgabe zugrunde, ein weiter entwickeltes Verfahren für ein Spam-Filter, das mit weißen Listen in der zuvor beschriebenen Art arbeitet, bereitzustellen, bei welchem die genannten Nachteile vermieden werden.

Diese Aufgabe löst die Erfindung dadurch, dass akzeptable Absender-Identifikationsangaben betreffende Einträge in der Datenbank automatisch erzeugt werden, indem Identifikationsangaben an das Datennetzwerk angeschlossener Computer zumindest als Bestandteile von akzeptablen Absender-Identifikationsangaben in der Datenbank gespeichert werden, wenn ein an diese Computer gerichteter ausgehender Datenverkehr registriert wird.

Die Grundidee der Erfindung ist es demnach, das Verhalten von Internetnutzern automatisiert zu überwachen, wobei aus dem Datenverkehr, der durch die Aktivitäten der Nutzer entsteht, darauf geschlossen wird, von welchen Absendern E-Mails akzeptiert werden sollen.

Das erfindungsgemäße Verfahren hat den Vorteil, dass die automatisierte Versendung von Bestätigungs-E-Mails, wie sie bei bekannten Spam-Filtern zur Erzeugung von Eintragungen in die entsprechenden weißen Listen erforderlich ist, vermieden werden kann. Es genügt die Analyse des ausgehenden Datenverkehrs, um die benötigten Einträge in die elektronische Datenbank zu erzeugen. Ein weiterer Vorteil ist, dass durchaus erwünschte E-Mails von Internet-Servern, wie beispielsweise Bestellbestätigungen bei E-Commerce-Geschäften, das Spam-Filter passieren können, da gemäß der Erfindung anhand des ausgehenden Datenverkehrs während des über das Datennetzwerk erfolgenden Bestellvorganges die akzeptable Absender-Identifikationsangabe des Servers automatisch ermittelt und in der Datenbank gespeichert wird.

Gemäß der Erfindung können sinnvollerweise Empfänger-Identifikationsangaben ausgehender elektronischer Nachrichten als akzeptable Absender-Identifikationsangaben in der Datenbank gespeichert werden. Wenn also ein Internet-Nutzer eine E-Mail versendet, so wird automatisch die E-Mail-Adresse des Empfängers als akzeptable Absenderadresse in der weißen Liste gespeichert. Somit entfällt für diejenigen Empfänger, die bereits eine E-Mail von

dem Internet-Nutzer erhalten haben, die Notwendigkeit, den zeitraubenden und aufwendigen Bestätigungsvorgang zur Erzeugung des Eintrags in die weiße Liste durchzuführen. Denkbar ist es, als Ergänzung des erfindungsgemäßen Verfahrens trotzdem eine automatisierte Bestätigung immer noch vorzusehen, falls eine elektronische Nachricht von einem noch nicht als akzeptabel registrierten E-Mail-Versender eingeht.

Sinnvoll ist es ferner, wenn bei dem erfindungsgemäßen Verfahren die Identifikationsangabe eines an das Datennetzwerk angeschlossenen Server-Computers in der Datenbank als Bestandteil einer akzeptablen Absender-Identifikationsangabe gespeichert wird, wenn in dem ausgehenden Datenverkehr die Anforderung eines Dienstes von diesem Server-Computer über das Datennetz registriert wird. Diese Ausgestaltung des erfindungsgemäßen Spam-Filters betrifft beispielsweise den oben angesprochenen Datenverkehr im Rahmen von E-Commerce-Geschäften. Während des Bestellvorgangs kann anhand des ausgehenden Datenverkehrs festgestellt werden, dass von einem Internet-Nutzer ein Dienst des entsprechenden E-Commerce-Servers angefordert wird. So ist z. B. bei der Teilnahme an einer Internet-Auktion des Diensteanbieters eBay anhand des ausgehenden Datenverkehrs feststellbar, dass von dem Internet-Nutzer die Internet-Seite „www.ebay.com" aufgesucht wird. Als Identifikationsangabe im Sinne der Erfindung wird dann die Second-Level-Domainbezeichnung „ebay" registriert und in der weißen Liste des Spam-Filters gespeichert, sodass nach dem Bestellvorgang E-Mails, die die Domainangabe „ebay" als Bestandteil der Absenderadresse, wie z.B. „sender@ebay.com" oder auch „info@ebay.de", enthalten, das Spam-Filter passieren und den Internetnutzer wunschgemäß erreichen können.

Eine vorteilhafte Weiterbildung des erfindungsgemäßen Verfahrens besteht darin, dass ein automatisch erzeugter Eintrag einer akzeptablen Absender-Identifikationsangabe in der Datenbank nach Ablauf eines vorgebbaren Zeitintervalls gelöscht wird. Es kann ohne weiteres sein, dass von einem Internet-Nutzer - unter Umständen auch versehentlich - ausgehender Datenverkehr erzeugt wird, der an einen Server gerichtet ist, welcher Spam versendet. Gemäß der Erfindung würde die Identifikationsangabe eines solchen

Servers als Bestandteil einer akzeptablen Absender-Identifikationsangabe in der weißen Liste registriert. Um zu verhindern, dass Spam von einem solchen Server dauerhaft zugestellt wird, kann vorgesehen sein, dass die Identifikationsangaben in der weißen Liste nach Ablauf eines vorgebbaren Zeitintervalls gelöscht werden.

Sinnvoll ist es des Weiteren, wenn die Absender-Identifikationsangaben in codierter Form in der Datenbank gespeichert werden. Ansonsten könnte die Arbeitsweise des erfindungsgemäßen Spam-Filters dazu missbraucht werden, den von einem Internetnutzer verursachten Datenverkehr auszuspionieren, um beispielsweise das „Surf-Verhalten" des Nutzers im Internet zu analysieren. Besonders sinnvoll ist es daher, ein bekanntes Einweg-Codierungsverfahren für die Codierung der Einträge in der Datenbank vorzusehen, sodass zwar der Vergleich der Absenderadressen eingehender E-Mails mit den in der weißen Liste gespeicherten akzeptablen Adressen möglich ist, die akzeptablen Adressen selbst aber nicht aus dem Datenbankinhalt rekonstruiert werden können.

Das erfindungsgemäße Verfahren kann ohne weiteres auf den Personalcomputern beliebiger Internetnutzer zum Einsatz kommen. Hierzu ist es zweckmäßig, dass Zugriffe auf Server-Computer über das Datennetzwerk mittels eines Anwendungsprogramms automatisch protokolliert werden und der ausgehende Datenverkehr zur Erzeugung von Einträgen in der Datenbank anschließend anhand des Protokolls analysiert wird. Durch eine geeignete Programmierung eines üblichen Browser-Programms zum Zugriff auf Server im Internet kann die Erzeugung des Protokolls gesteuert werden. Ein in geeigneter Weise angepasstes E-Mail-Programm kann dann durch Auswertung des Protokolls die akzeptablen Absender-Identifikationsangaben ermitteln und diese in die weiße Liste eintragen.

Alternativ besteht auch die Möglichkeit, das erfindungsgemäße Verfahren auf einem an das Datennetzwerk angeschlossenen Server zu implementieren, welcher den ein- und ausgehenden Datenverkehr weiterleitet. Dies hat insbesondere den Vorteil, dass die unerwünschten elektronischen Nachrichten frühzeitig abgefangen werden, sodass möglichst wenig Bandbreite für die

Übertragung dieser Nachrichten zu den einzelnen Internetnutzern verschwendet wird. Das gemäß der Erfindung arbeitende Spam-Filter kann beispielsweise auf einem so genannten Gateway-Computer oder auf einen Proxy-Server installiert werden. Auf einem Proxy-Server werden im Internet zur Verfügung stehende Dateninhalte (Web-Seiten) zwischengespeichert, um so eine effektivere Ausnutzung der Übertragungsbandbreite innerhalb des Datennetzwerkes zu ermöglichen. Mittels eines Proxy-Servers kann in besonders einfacher Weise in dem ausgehenden Datenverkehr die Anforderung eines Dienstes von einem beliebigen Internet-Server registriert werden, was zur Implementierung des erfindungsgemäßen Spam-Filters ausgenutzt werden kann. Als weitere Alternative kann das erfindungsgemäße Filter auch einem so genannten Mail-Server, d.h. einem für die E-Mail-Übertragung zuständigen Server-Computer, eines Internet-Diensteanbieters vorgeschaltet sein, sodass bereits der Mail-Server von Spam entlastet wird.

Ein Ausführungsbeispiel der Erfindung wird im Folgenden anhand der Zeichnung erläutert. Die Zeichnung zeigt in Form eines Blockdiagramms die erfindungsgemäße Überwachung der Übertragung von elektronischen Nachrichten innerhalb eines Datennetzwerkes.

An ein globales Datennetzwerk 1, bei dem es sich beispielsweise um das Internet handeln kann, sind ein Server-Computer 2 sowie mehrere weitere Computer 3, 4 und 5 angeschlossen. Bei den Computern 3, 4 und 5 handelt es sich um die Personalcomputer von Internetnutzern. Des Weiteren ist an das Internet 1 ein Server-Computer 6 eines Internet-Diensteanbieters angeschlossen. Bei dem Server-Computer 6 handelt es sich um einen so genannten Mail-Server, der dazu dient, über das Internet 1 eingehende elektronische Nachrichten, d. h. E-Mails an die Kunden des Internet-Diensteanbieters weiterzuleiten. Mit dem Mail-Server 6 stehen dem Kunden des Internet-Diensteanbieters zugeordnete Personalcomputer 7, 8 und 9 in Verbindung. Auf dem Mailserver 6 läuft ein Programm 10, welches nach dem erfindungsgemäßen Verfahren arbeitet. Von dem Programm 10 werden Absender-Identifikationsangaben, d. h. Absenderadressen, von auf dem Server 6 eingehenden E-Mails ermittelt. Es erfolgt dann die Abfrage einer elektronischen Datenbank 11 und eine Überprüfung, ob die ermittelte Absenderadresse in der

Datenbank 11 als akzeptable oder nicht-akzeptable Absenderadresse registriert ist. In Abhängigkeit vom Ergebnis der Überprüfung werden die eingehenden E-Mails entweder verworfen oder in Postfächern 12, 13 und 14, die den Computern 7, 8 und 9 zugeordnet sind, gespeichert. Mittels des Programms 10 werden akzeptable Absenderadressen automatisch ermittelt und in der Datenbank 11 gespeichert. Hierzu werden die Identifikationsangaben der an das Datennetzwerk 1 angeschlossen Computer 2, 3, 4 und 5, d. h. die diesen Computern zugeordneten E-Mail-Adressen bzw. deren Domain-Bezeichnungen, als akzeptable Absenderadressen in der Datenbank 11 in Form einer weißen Liste gespeichert, wenn ein an diese Computer 2, 3, 4 und 5 gerichteter Datenverkehr, der von den Computern 7, 8 oder 9 ausgeht, registriert wird.

Wenn beispielsweise von dem Computer 7 eine E-Mail über den Mailserver 6 und über das Internet 1 an den Computer 3 verschickt wird, so registriert das Programm 10 die Empfängeradresse der ausgehenden E-Mail und speichert diese als akzeptable Absenderadresse in der Datenbank 11. Wenn zu einem späteren Zeitpunkt eine E-Mail von dem Computer 3 an den Computer 7 verschickt wird, so kann diese E-Mail das durch das Programm 10 implementierte Spam-Filter passieren, da die Absenderadresse der E-Mail als akzeptable Absenderadresse in der Datenbank 11 gespeichert ist.

Falls es sich bei dem Server-Computer 2 um einen Spammer handelt, so werden von dem Spammer 2 ausgehende E-Mails von dem Mailserver 6 nicht weitergeleitet, da das Programm 10 nach einer Abfrage der Datenbank 11 die Absenderadresse des Servers 2 nicht als akzeptable Absenderdresse verifizieren kann.

Außerdem überwacht das Programm 10 den ausgehenden Datenverkehr hinsichtlich der Anforderung von Diensten von an das Datennetz 1 angeschlossenen Computern. Wenn beispielsweise der Computer 9 eine auf dem Computer 5 abgespeicherte Internet-Seite abruft, so wird die dem Computer 5 zugeordnete Domainbezeichnung, oder zumindest ein Bestandteil der selben, automatisch von dem Programm 10 als akzeptable Absenderadresse in der Datenbank 11 gespeichert. Wenn zu einem späteren Zeitpunkt von dem Computer 5 eine E-Mail an den Computer 9 verschickt wird, so kann

diese E-Mail das gemäß der Erfindung arbeitende Spam-Filter passieren, da das Programm 10 die Domainbezeichnung des Computers 5 durch Zugriff auf die Datenbank 11 als akzeptable Absenderadresse identifiziert.

Gemäß der Erfindung wird letztlich der von den Computern 7, 8 und 9 generierte Datenverkehr mittels des Servers 6, auf dem das Programm 10 läuft, überwacht, um anhand des ausgehenden Datenverkehrs akzeptable Absenderadressen zu ermitteln, die mittels der Datenbank 11 in Form einer weißen Liste gespeichert werden. Falls die Absenderadresse einer auf dem Server 6 eingehenden E-Mail mit einer in der Datenbank 11 gespeicherten Adresse übereinstimmt, so wird diese E-Mail nicht als Spam angesehen und an die entsprechenden Empfänger weitergeleitet.

- Ansprüche -

Patentansprüche

1. Verfahren zur computergestützten Überwachung der Übertragung von elektronischen Nachrichten innerhalb eines Datennetzwerkes (1), mit den folgenden Verfahrensschritten:

a) Ermittlung einer Absender-Identifikationsangabe einer eingehenden elektronischen Nachricht,

b) Abfrage einer elektronischen Datenbank (11) und Überprüfung, ob die Absender-Identifikationsangabe in der Datenbank (11) als akzeptable oder nicht-akzeptable Absender-Identifikationsangabe registriert ist,

c) Übermittlung der elektronischen Nachricht in Abhängigkeit vom Ergebnis der Überprüfung im Verfahrensschritt b),

d a d u r c h g e k e n n z e i c h n e t , dass akzeptable Absender-Identifikationsangaben betreffende Einträge in der Datenbank (11) automatisch erzeugt werden, indem Identifikationsangaben an das Datennetzwerk (1) angeschlossener Computer (2, 3, 4, 5) zumindest als Bestandteile von akzeptablen Absender-Identifikationsangaben in der Datenbank (11) gespeichert werden, wenn ein an diese Computer (2, 3, 4, 5) gerichteter ausgehender Datenverkehr registriert wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass Empfänger-Identifikationsangaben ausgehender elektronischer Nachrichten als akzeptable Absender-Identifikationsangaben in der Datenbank (11) gespeichert werden.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Identifikationsangabe eines an das Datennetzwerk angeschlossenen Server-Computers (2) in der Datenbank (11) als Bestandteil einer akzeptablen

Absender-Identifikationsangabe gespeichert wird, wenn in dem ausgehenden Datenverkehr die Anforderung eines Dienstes von diesem Server-Computer (2) über das Datennetz (1) registriert wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass ein automatisch erzeugter Eintrag einer akzeptablen Absender-Identifikationsangabe in der Datenbank (11) nach Ablauf eines vorgebbaren Zeitintervalls gelöscht wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Absender-Identifikationsangaben in codierter Form in der Datenbank (11) gespeichert werden.

6. Verfahren nach einem der Ansprüche 3 bis 5, dadurch gekennzeichnet, dass Zugriffe auf Server-Computer (2) über das Datennetzwerk mittels eines Anwendungsprogramms (10) automatisch protokolliert werden und der ausgehende Datenverkehr zur Erzeugung von Einträgen in der Datenbank (11) anschließend anhand des Protokolls analysiert wird.

7. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass das Verfahren auf einem an das Datennetzwerk angeschlossenen Server (6) implementiert ist, welcher den ein- und ausgehenden Datenverkehr weiterleitet.